Install the EH1000v/2000v/ECM with Hyper-V

Publication Date: 9/10/2015

Contents

How Mirroring Works

ExtraHop is a passive system.

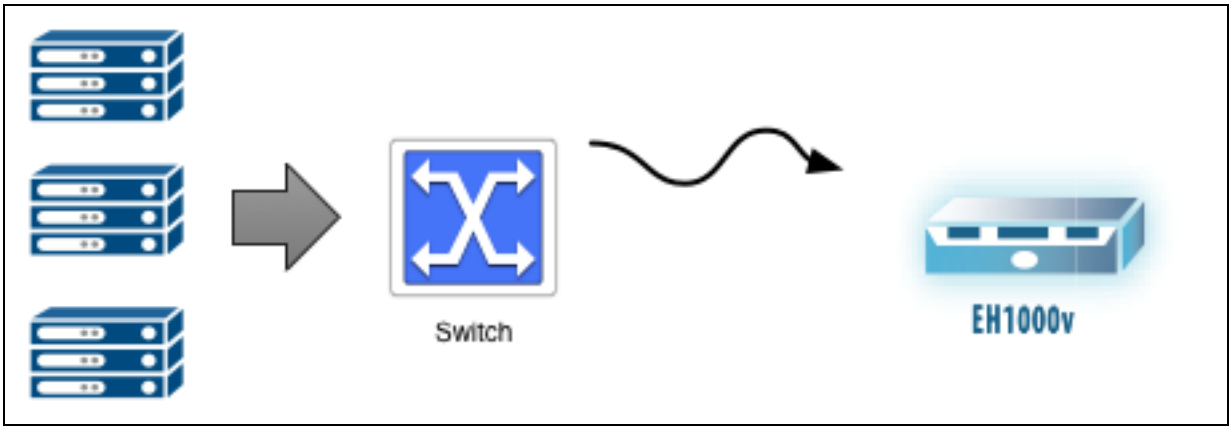
Its wire data feed comes entirely from mirrored traffic. This is an improvement from traditional methods of collecting wire data with packet analyzers. With ExtraHop, the traffic is mirrored directly into the appliance and then reassembled into full per-client sessions and transaction streams, offering you the entire transaction payload in real time to analyze. There are two ways to mirror traffic into ExtraHop: network-based mirroring and host-based mirroring. This topic discusses the differences between the two.

Network-Based Mirroring

The big advantage with network based mirroring is that you can set it up at the network level, capturing traffic from multiple hosts with a minimum amount of configuration. There are different types of network-based mirroring, each designed for mirroring traffic to a target in a particular situation. The big challenge with all the network-based mirroring strategies is that they rely heavily on the capabilities of the hardware on your network (physical or virtual). If you're running a virtual ExtraHop appliance, the hypervisor you're running (and even the version of hypervisor) also plays into the equation. That said, if you can take advantage of network-based mirroring you'll probably want to because once it's set up, it requires less administrative effort to maintain.

There are three main types of network-based mirroring.

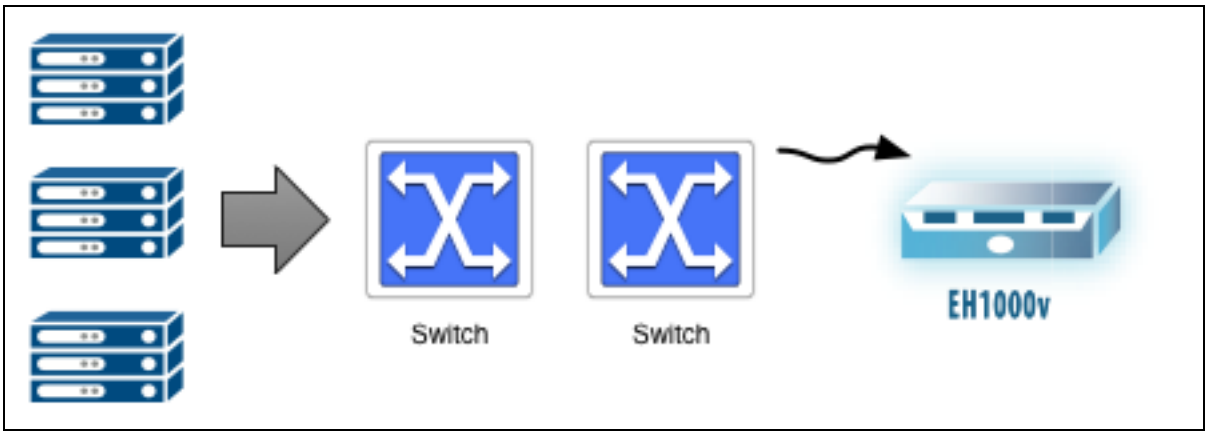
SPAN



The SPAN port is the name of the port on Cisco switches that mirrors traffic. SPAN stands for Switched Port ANalyzer (SPAN). Different vendors use different names, but spanning has become synonymous for a port on a switch that mirrors traffic. The key thing about a SPAN is that it's all local traffic. You can configure any of the ports on the switch to mirror traffic to an ExtraHop appliance that has access to the SPAN port.

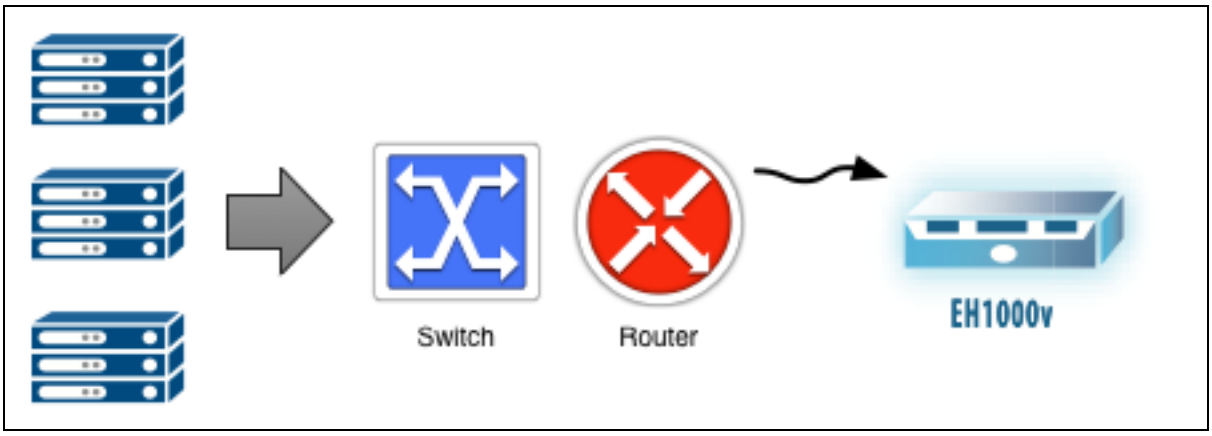
Promiscuous mode is similar to SPAN, but instead of mirroring only select local port traffic to the SPAN port, promiscuous mode mirrors all the traffic from every port. Any traffic that comes through the switch is mirrored to your ExtraHop appliance.

RSPAN



RSPAN is useful if the traffic you're interested in mirroring is more than one switch away from where you can attach your ExtraHop appliance. The "R" in RSPAN stands for remote. You're spanning all the traffic from one switch through any number of additional switches to your target ExtraHop appliance using a dedicated mirroring VLAN. Each switch in the path needs to be configured to carry the dedicated VLAN that contains the mirror traffic.

ERSPAN

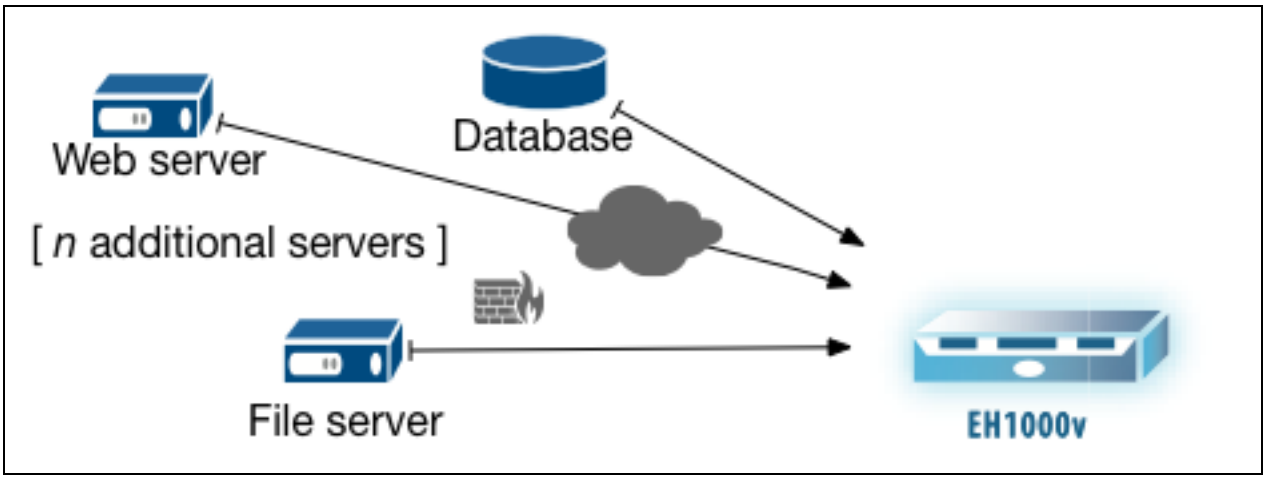


If a Layer 3 (L3) boundary (such as a Router, Firewall, or Layer 3 Switch) sits between the traffic you're interested in mirroring and where you can attach your ExtraHop appliance, ERSPAN may be helpful to you. To cross the Layer 3 boundary, ERSPAN encapsulates the mirror traffic in a GRE tunnel addressed to the IP address of a capture interface on the ExtraHop appliance. The encapsulated mirror traffic navigates the network just as any other packet would.

Host-Based Mirroring

If network-based mirroring won't work for you, then host-based mirroring is a reliable way to get traffic into ExtraHop.

Software Tap



Host-based mirroring requires that you install a software tap on each host you want to monitor. The big advantage of the software tap is that it works with any type of network gear you have. It works independent of the type or version of hypervisor you're running. Host-based mirroring is a way of configuring the adapter on a host to duplicate and forward all traffic to ExtraHop. You can install it on Windows or Linux hosts.

The software tap (also called RPCAP and a packet forwarder) is analogous to a network tap, which is an unobtrusive hardware device for mirroring traffic from a network.

Installation Requirements

This section includes hardware and software requirements for the host on which you are installing the ExtraHop virtual appliance.

System Requirements: EH1000v

Installation has the following requirements:

- An existing installation of Hyper-V on Windows Server 2012 (or later)
- A Hyper-V Manager client

The following server hardware is required for the EH1000v:

- **Processor**: 2 processing cores with hyper-threading support, VT-x technology, and 64-bit architecture
  To use SSL decryption, three processing cores are required. Refer to *ExtraHop Guide: Adding a CPU Core to the EH1000v with Hyper-V* for more information.
- **Memory**: 4 GB or higher
- **Disk**: 46 GB or higher (thick-provisioned)
- **Network**: You can configure the EH1000v to monitor intra-VM or external traffic.
  - **Intra-VM**: One 1-Gbps Ethernet network port is required (for management). The management port must be accessible on port 443.
  - **External**: Two 1-Gbps Ethernet network ports are required for the physical port mirror and management. The physical port mirror interface must be connected to the port mirror of the switch. While it is possible to use a 10-Gbps Ethernet network port for the port mirror interface, it is not recommended as the virtual appliance cannot process more than 1 Gbps of traffic.
- **Registration**: For registration purposes, the EH1000v requires outbound DNS connectivity on UDP port 53 unless managed by the ExtraHop Central Manager (ECM).

System Requirements: EH2000v

Installation has the following requirements:

- An existing installation of Hyper-V on Windows Server 2012 (or later)
- A Hyper-V Manager client

The following server hardware is required for the EH2000v:

- **Processor**: 6 processing cores with hyperthreading support, VT-x technology, and 64-bit architecture
  To use SSL decryption, three processing cores are required. Refer to *ExtraHop Guide: Adding a CPU Core to the EH1000v with Hyper-V* for more information.
- **Memory**: 6 GB or higher
- **Disk**: 255 GB or higher (thick-provisioned)
- **Network**: You can configure the EH2000v to monitor intra-VM or external traffic.
  - **Intra-VM**: One 1-Gbps Ethernet network port is required (for management). The management interface must be accessible on port 443.
  - **External**: Two to four 1-Gbps Ethernet network ports are required for the physical port mirror and management. The physical port mirror interface must be connected to the port mirror of the switch. While it is possible to use a 10-Gbps Ethernet network port for the port mirror interface, it is not recommended as the virtual appliance cannot process more than 3 Gbps of traffic.
- **Registration**: For registration purposes, the EH2000v requires outbound DNS connectivity on UDP port 53 unless managed by the ExtraHop Central Manager (ECM).

System Requirements: ECM

The following table is a guideline to achieve optimal performance with the ExtraHop Central Manager (ECM). These are minimum requirements that you may need to adjust depending on the size of your virtual machine.

Number of ExtraHop nodes to manage:	1-4	5-16	17-64	65 or more
Required CPU cores	2	4	8	16
Required RAM	4 GB	8 GB	16 GB	24 GB

Regardless of the number of nodes you want to manage, your environment must also meet the following requirements

- 44 GB hard disk
- One 1 Gbps Ethernet network port accessible on port 443 (for management)
- An ExtraHop virtual appliance license key

Note: The ECM does not require any port mirroring or special virtual networking configuration.

Installing the ExtraHop VM

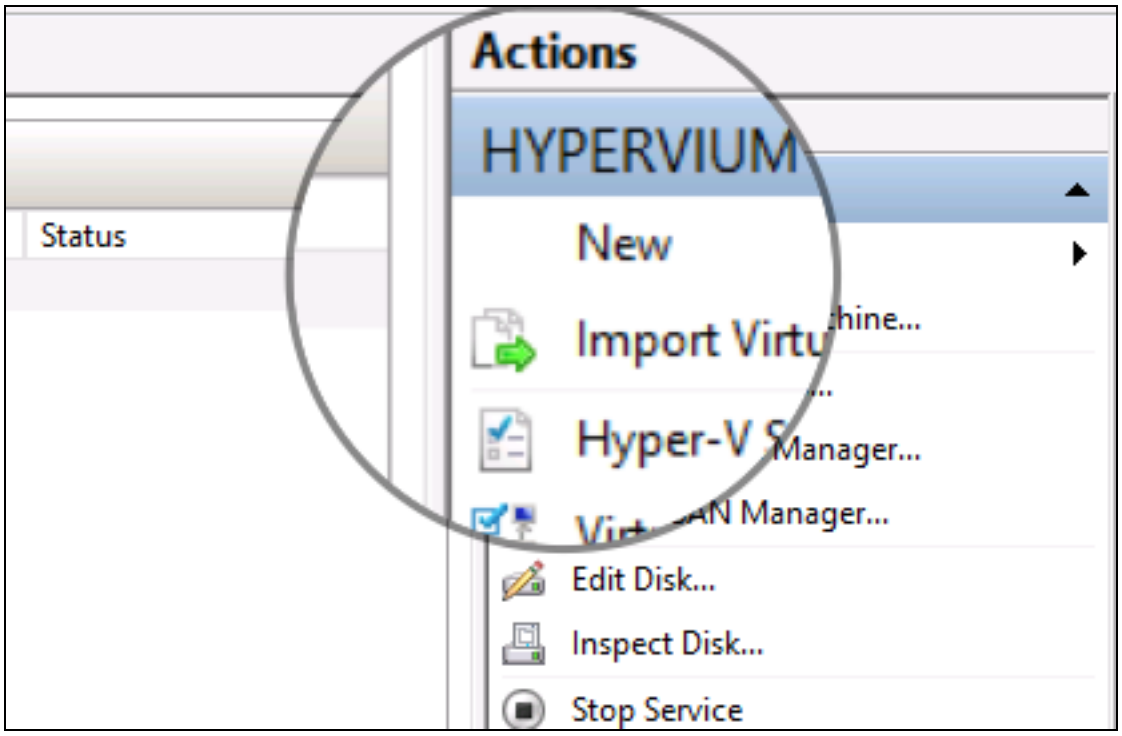
Before you install the ExtraHop virtual appliance, ensure the following:

- You have downloaded the file for the ExtraHop virtual appliance (this is an OVA file for OVA-aware hypervisor products). If you have not downloaded the file, contact support@extrahop.com.
- You have the ExtraHop virtual appliance license key provided by ExtraHop. If you do not have a license key, contact support@extrahop.com.
- You have an existing installation of one of the following virtualization products:
  - Microsoft Hyper-V
- Your host system meets the minimum hardware requirements, and you understand the disk requirements for setting up an ExtraHop appliance.
- If you are using a software tap, you have administrative access to servers you want to monitor, and you are running a 64-bit operating system (Linux/Windows). If you are using Windows, you must be using Windows Server 2008 R2 or Windows Server 2012 (or later).
- If you want to use Port Mirroring mode, you have administrative access to any physical or virtual switches that require configuration.

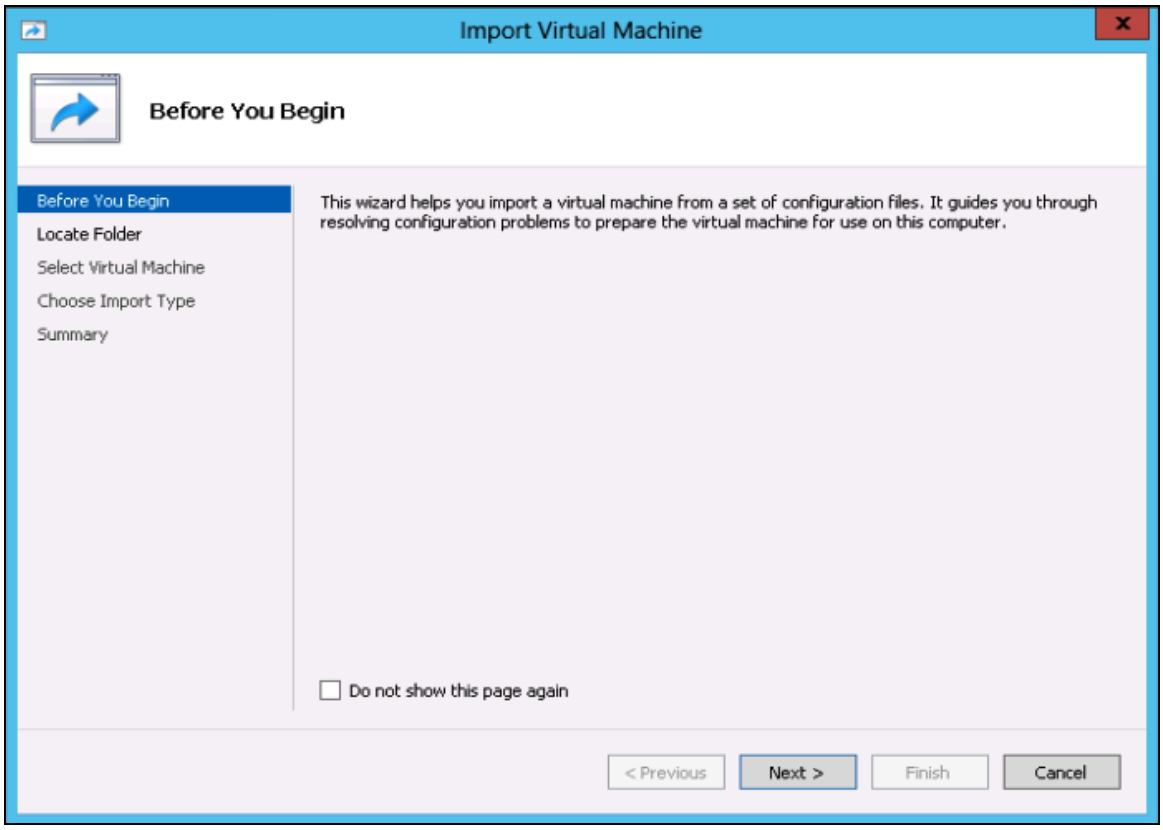
Installing the Files for Hyper-V

To install the files to run the ExtraHop virtual appliance with Hyper-V, complete the following steps.

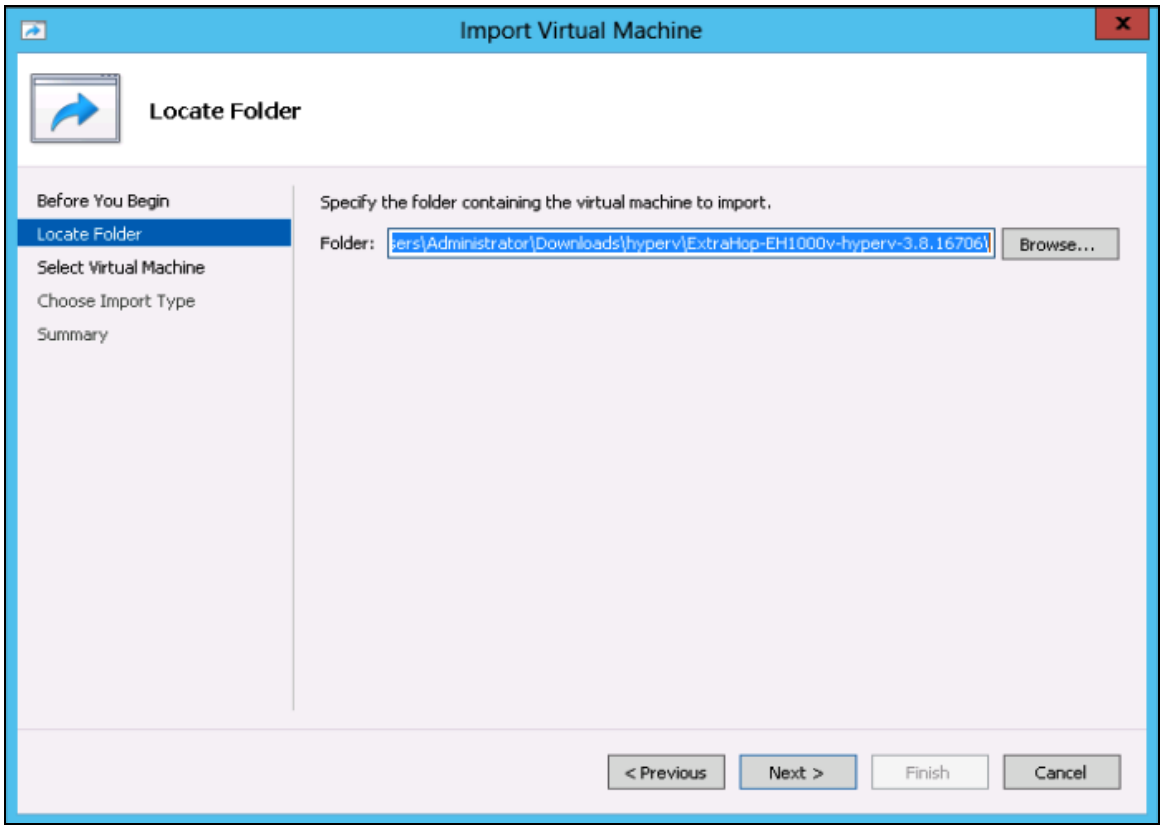
1. Go to the **Start** menu and open the **Hyper-V Manager**.
2. In the right pane of the Hyper-V Manager, click **New** and select **Import Virtual Machine...**.



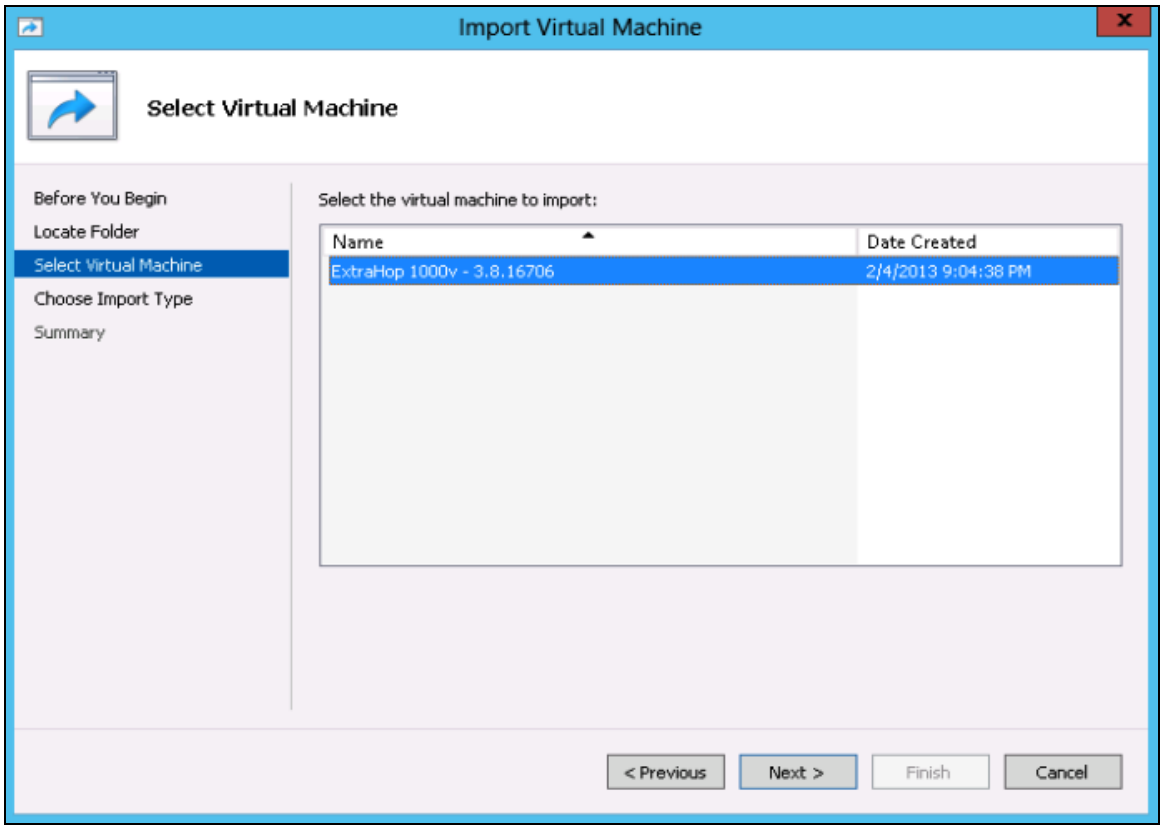
3. In the Import Virtual Machine Wizard, click **Next**.



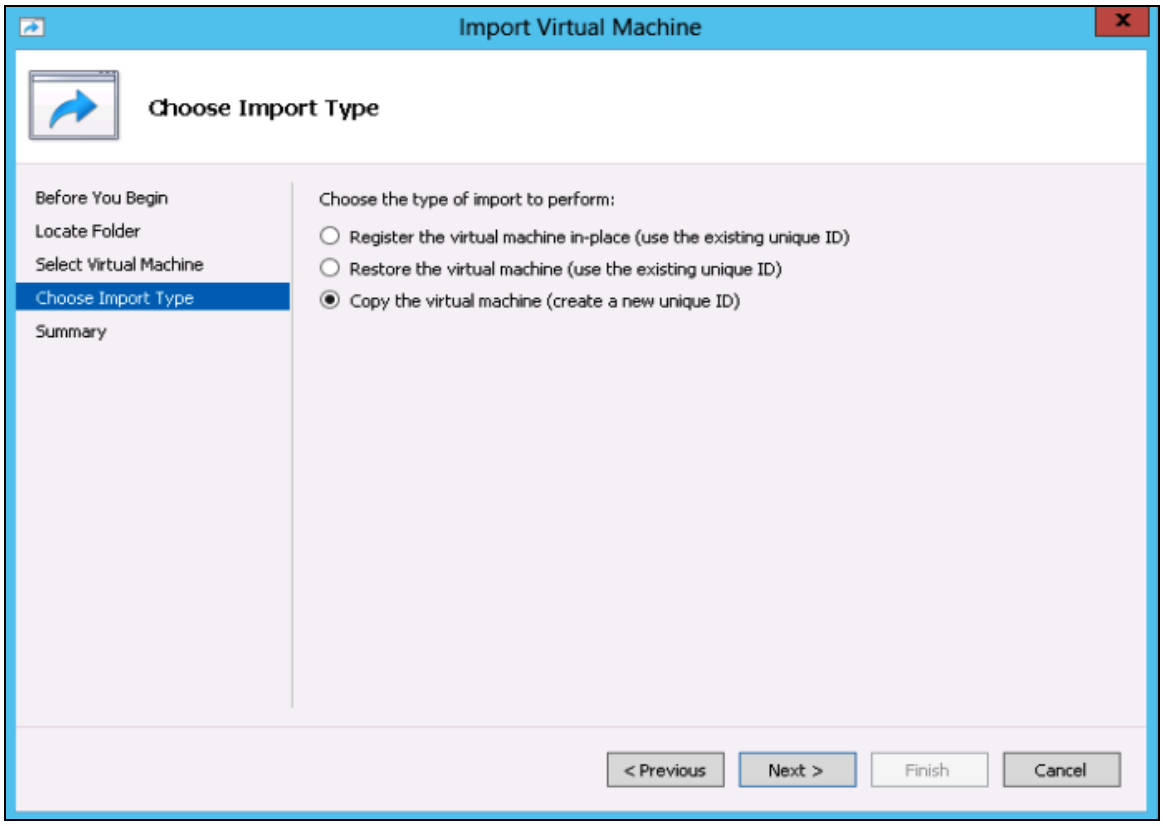
4. Browse to the folder with the extracted files and click **Next**.



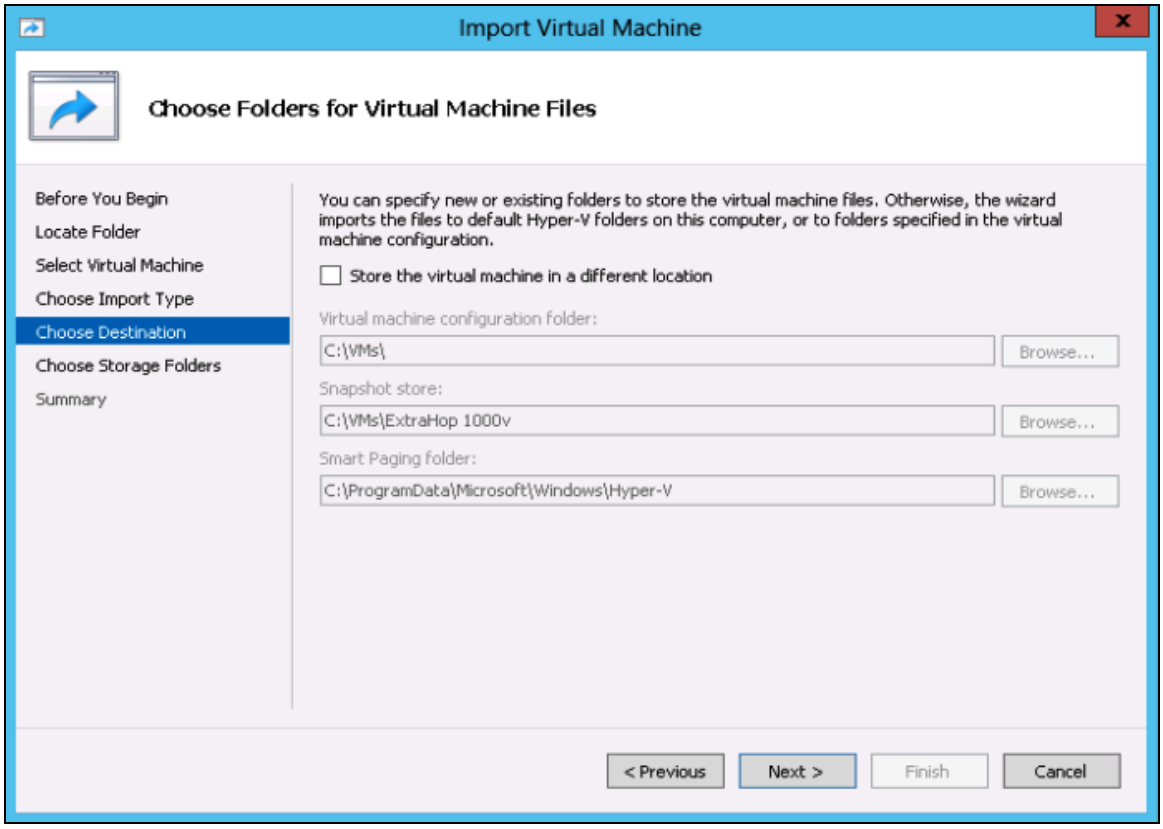
5. On **Select Virtual Machine**, click **Next**.



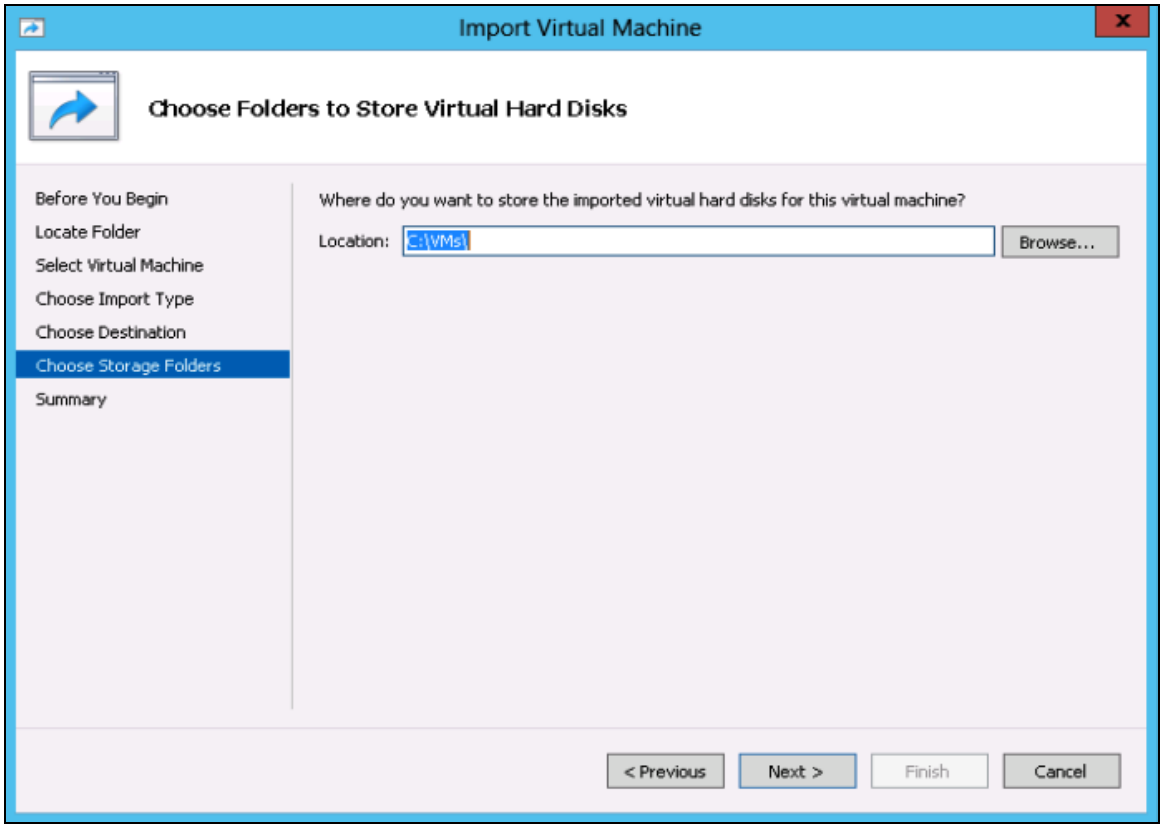
6. Select **Copy the virtual machine** and click **Next**.



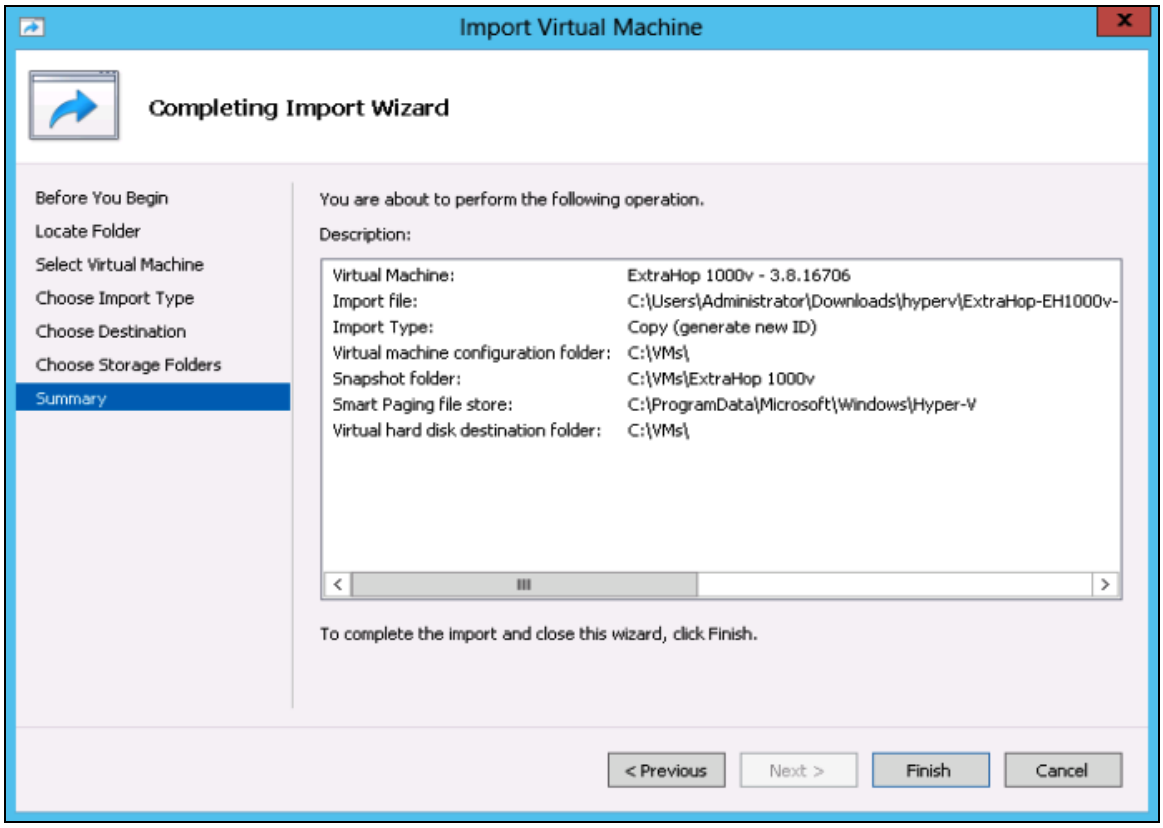
7. On **Choose Folders for Virtual Machine Files**, select the location to store the configuration of the VM and click **Next**.



8. On **Choose Storage Folders to Store Virtual Hard Disks**, select a location to store the virtual hard disks and click **Next**.

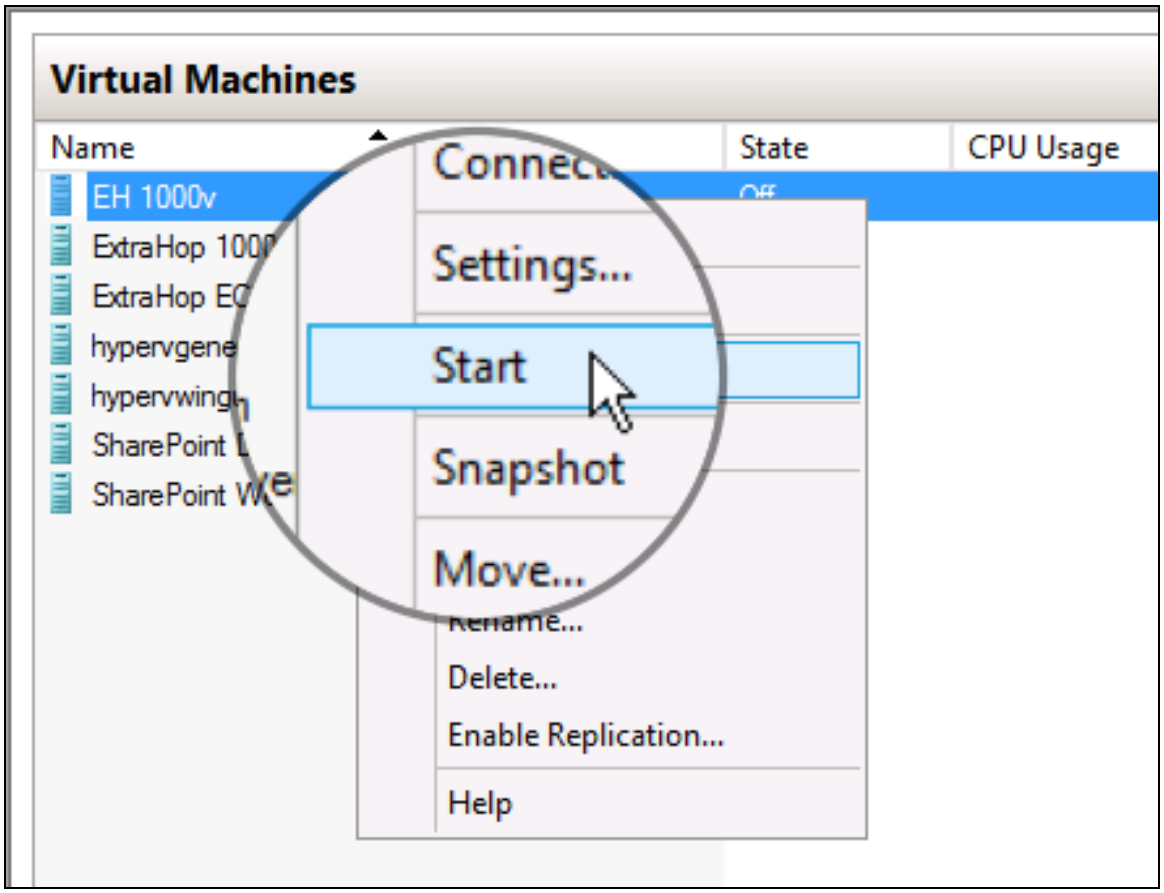


9. On the summary screen review your choices and then click **Finish**.

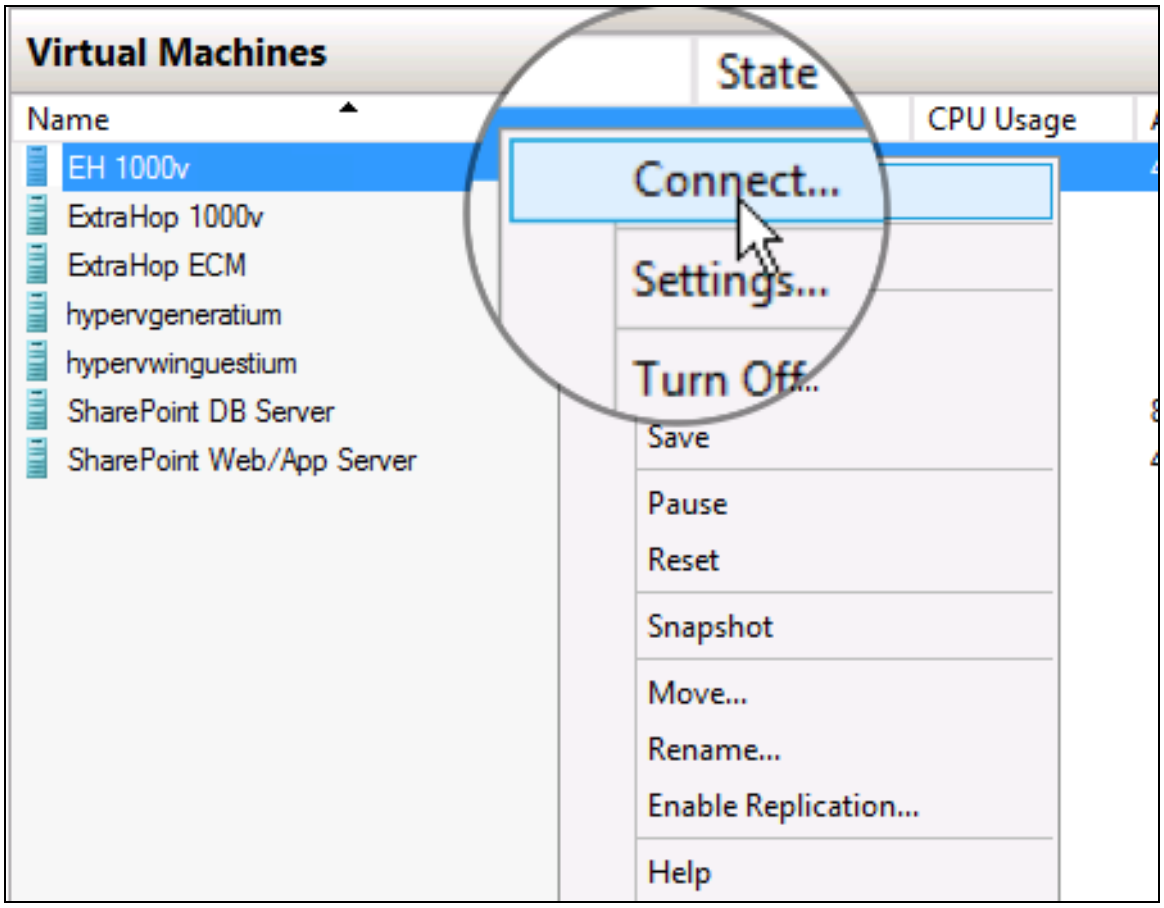


10. Wait several minutes for the files to copy.

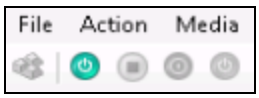
11. In the Virtual Machines list, right-click the virtual machine and select **Start**.



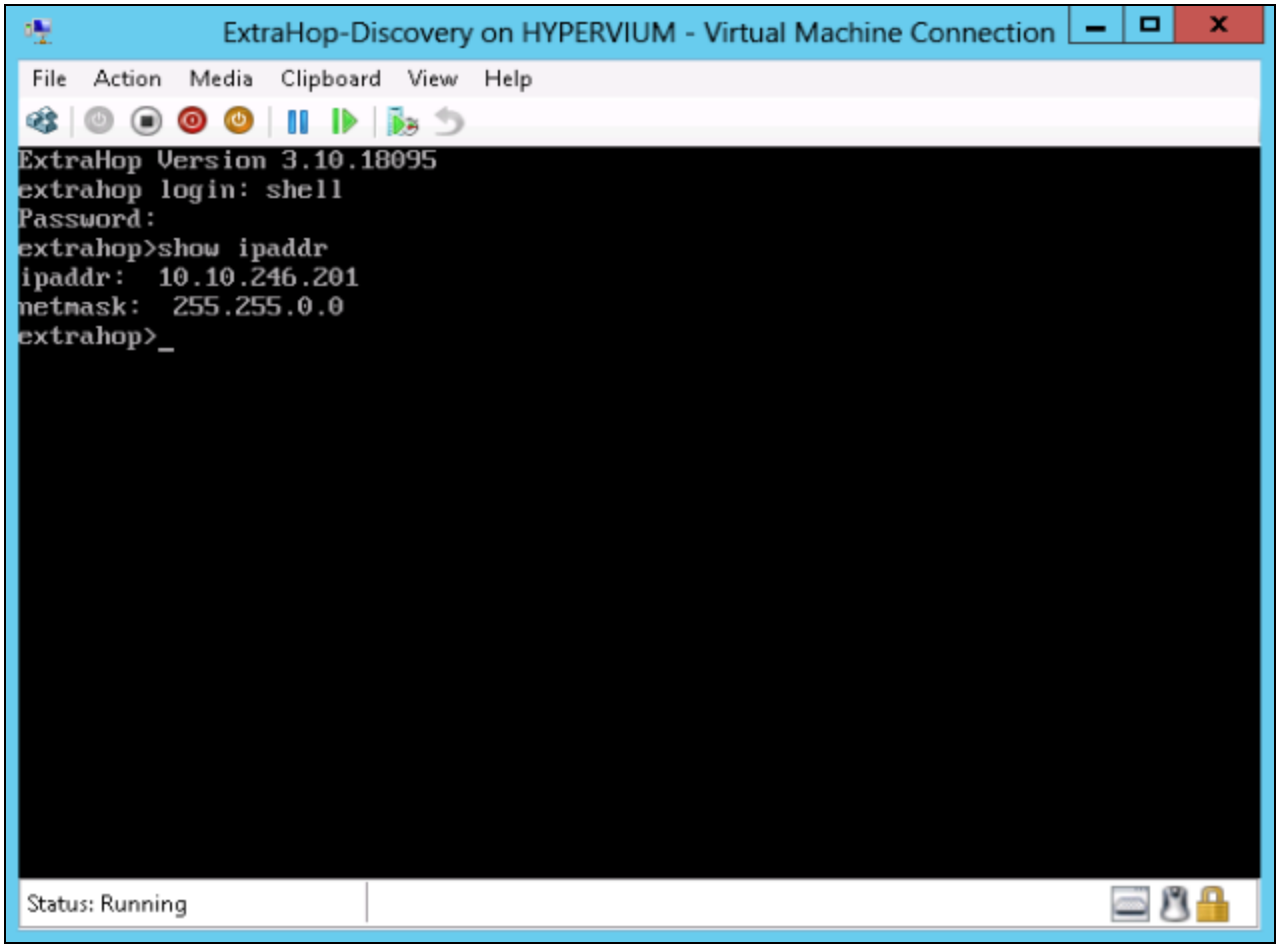
12. Right-click the virtual machine again and select **Connect**.



13. Click the green start button at the top of the screen and wait for the login prompt.



14. Run the `show ipaddr` command to display the IP address of the ExtraHop Discovery Edition.



If your network does not support DHCP, see **Configuring a Static IP Address** to set a static IP address.

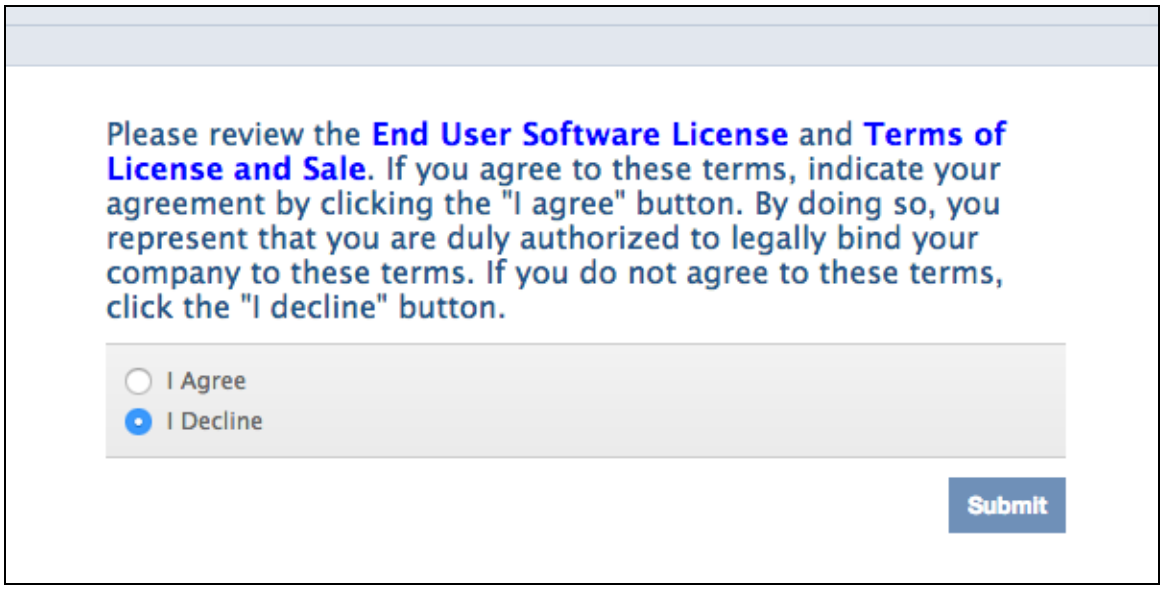
> **Note**: The default time server setting is `pool.ntp.org`. To configure the time servers manually, refer to the System Settings section of the *ExtraHop Admin UI Users Guide.*

15. You'll need the IP address to apply the ExtraHop license in the next procedure.

Applying the ExtraHop License

The ExtraHop virtual appliance requires a product key and a license in order to function.

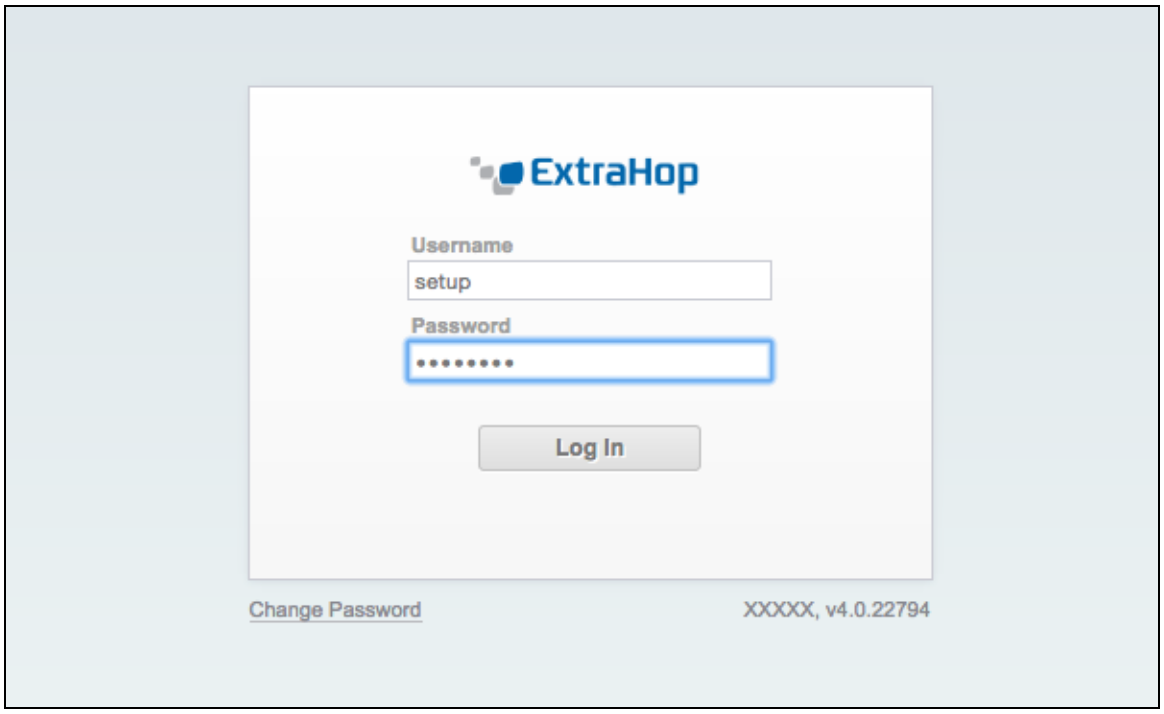
1. Browse to the ExtraHop appliance: (`https://<extrahop_management_ip>/admin`)



> If your browser prompts you about security certificates, ignore the warning and proceed.

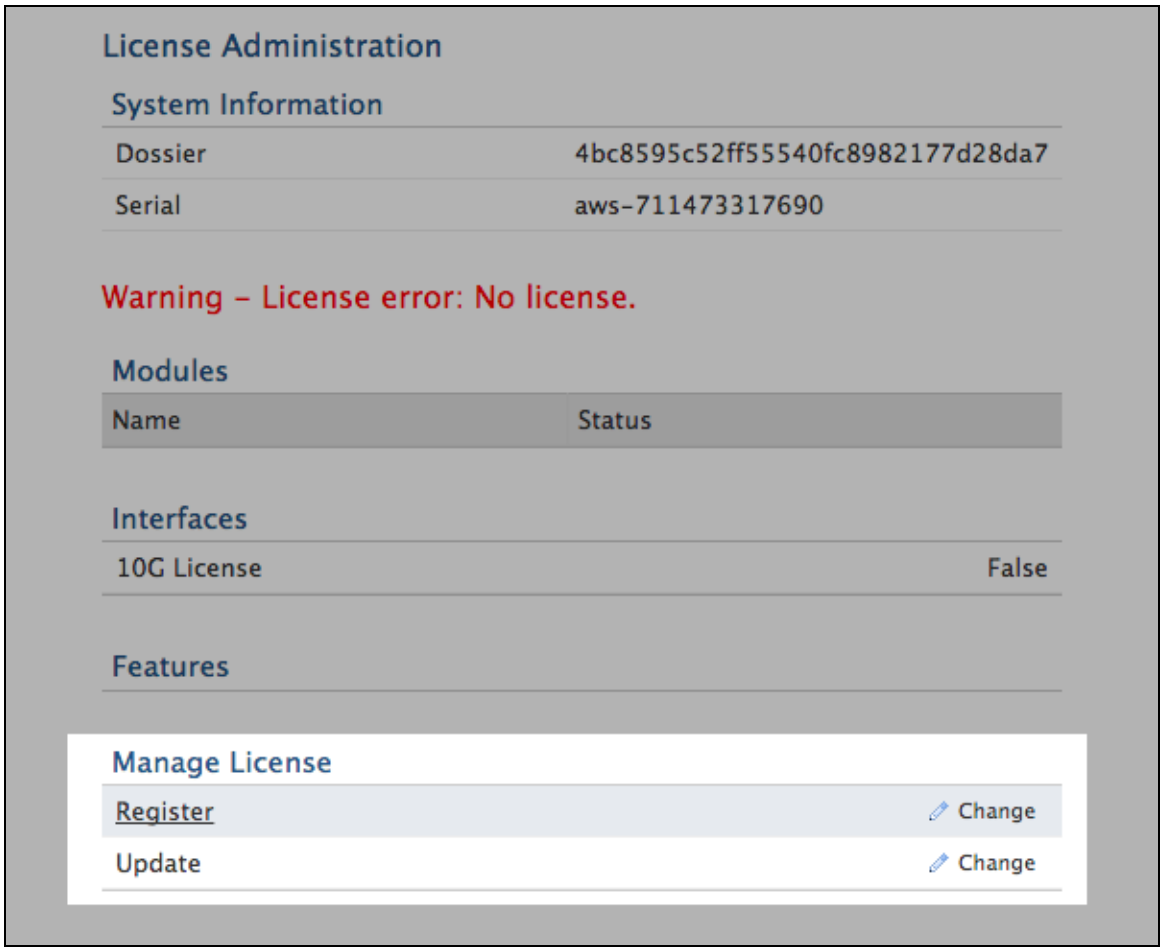
2. Review the license agreement, select **I Agree**, and click **Submit**.

3. On the login screen, enter the default user name and password:
   - **Username**: `setup`
   - **Password**: `default`

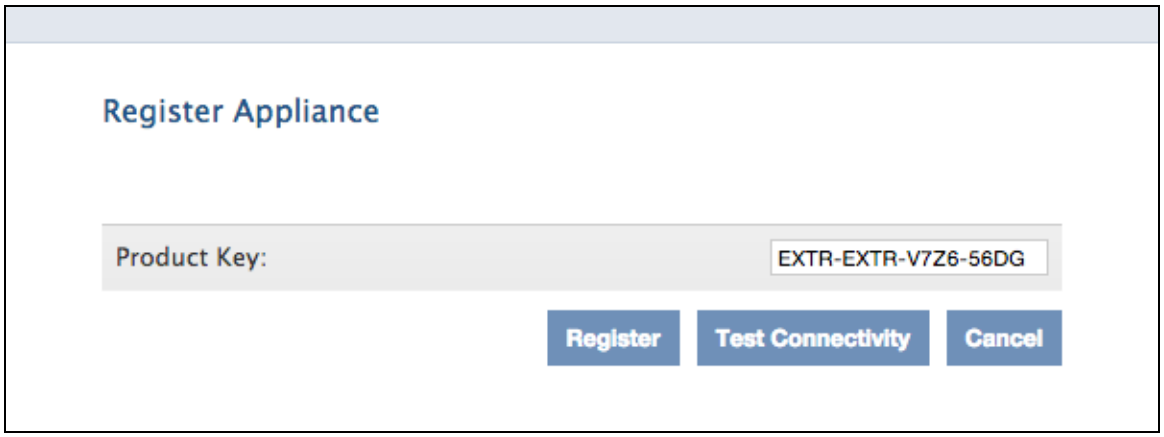


4. Click **ExtraHop Administration**.

5. Under **Manage License**, click **Register** to enter the product key.

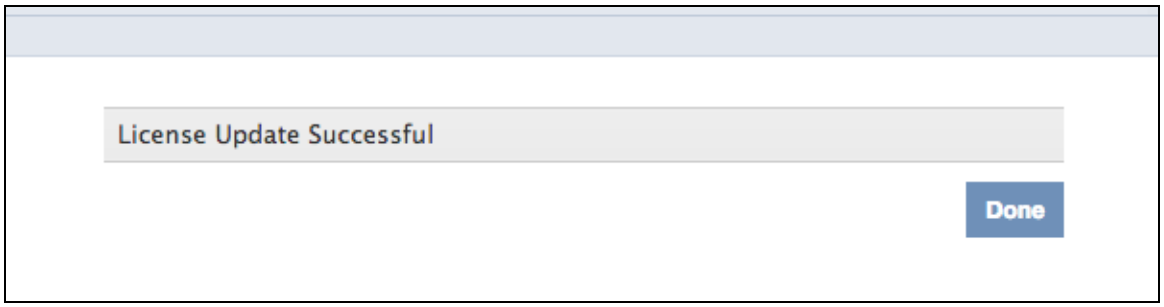


6. Enter the product key and then click **Register**.

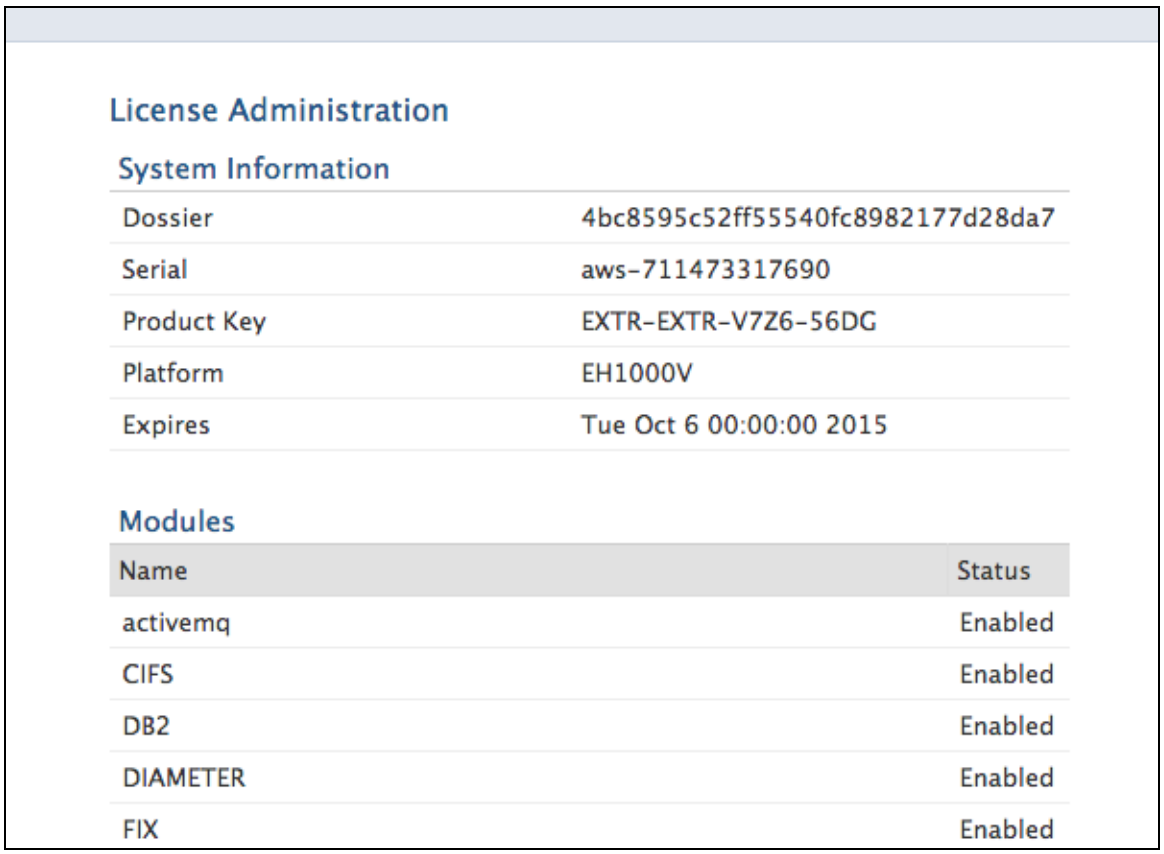


The ExtraHop system contacts the license server and validates the product key. After the product key is validated, the license is downloaded.

7. Click **Done**.



This is an example of the License Administration page showing a properly licensed ExtraHop system:



The ExtraHop system is now licensed and able to receive mirrored traffic.

Configuring a Static IP Address

The ExtraHop virtual appliance is delivered with DHCP enabled. If your network does not support DHCP, no IP address would be acquired, and you must configure a static address manually. To configure a static IP address, complete the following steps:

1. Log in to the console. Use the user account named *shell* and the password default.
2. Enable the privilege commands.

```
extrahop>enable
Password:default
extrahop#
```

3. Enter the configuration section.

```
extrahop#config
extrahop(config)#
```

4. Enter the interface section.

```
extrahop(config)#int
extrahop(config-if)#
```

5. Set the IP address and DNS using this syntax: `ip ipaddr IP_ADDRESS NETMASK GATEWAY DNS`.

```
extrahop(config-if)#ip ipaddr 10.10.10.10 255.255.0.0 10.10.1.254 8.8.8.8
```

6. Save the running config.

```
extrahop(config-if)#exit
extrahop(config) * #running_config save
Would you like to write configuration changes to default config [Y/n]?: y
extrahop(config)#
```

The full set of commands is as follows:

```
extrahop>enable
Password:
extrahop#config
extrahop(config)#int
extrahop(config-if)#ip ipaddr 10.10.10.10 255.255.0.0 10.10.1.254 8.8.8.8
Changing IP address. Please wait...
.Done
extrahop(config-if)# exit
extrahop(config) * #running_config save
Would you like to write configuration changes to default config [Y/n]?: y
extrahop(config)#
```

Note: The default time server setting is `pool.ntp.org`. To configure the time servers manually, refer to the **System Settings** section of the *ExtraHop Admin UI Users Guide*.

Mirror Wire Data

This section includes procedures for mirroring data to your ExtraHop virtual appliance.

Mirroring Internal and External Traffic

The ExtraHop virtual appliance can be configured to monitor network traffic in the following network configuration examples. Each example requires a modification to the network configuration of its hypervisor host and uses Network Adapter 1 as the management interface.

- **Monitoring Intra-VM Traffic**
- **Monitoring External Mirrored Traffic to the VM**

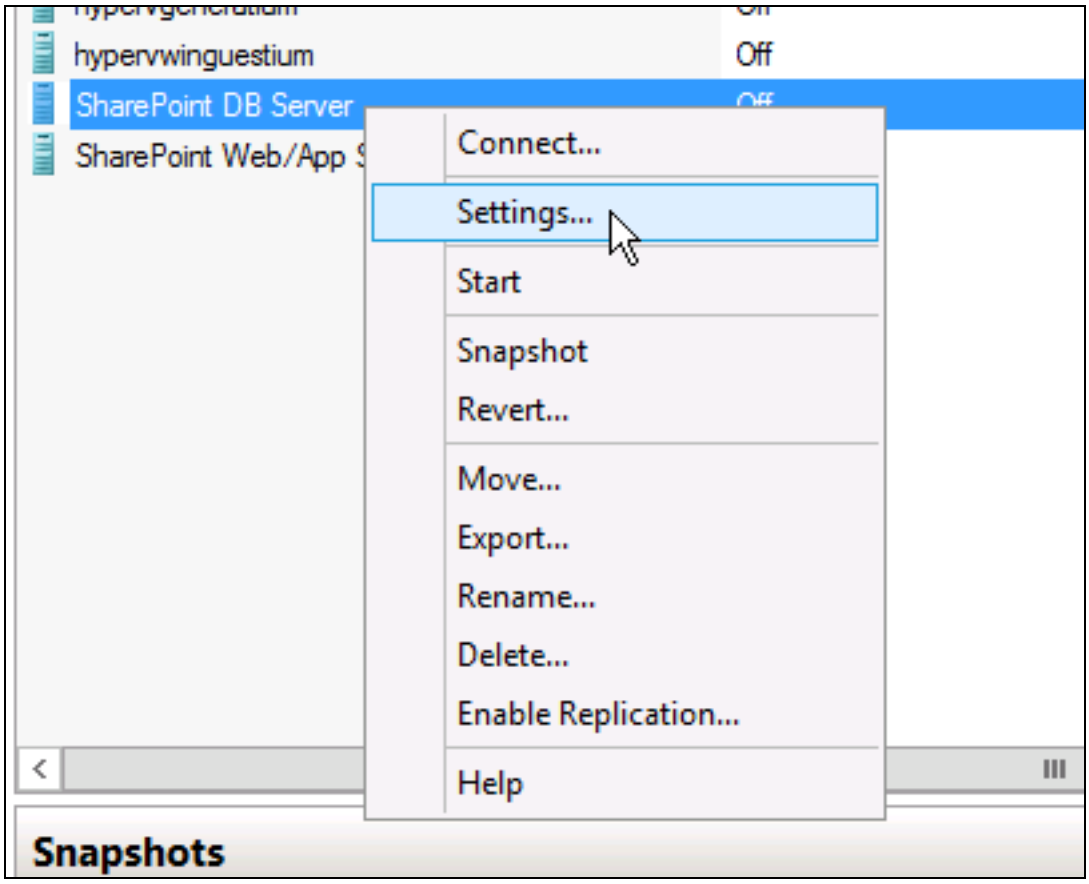
Note: Monitoring external network-mirrored traffic requires an external NIC and an associated virtual switch.

Monitoring Intra-VM Traffic

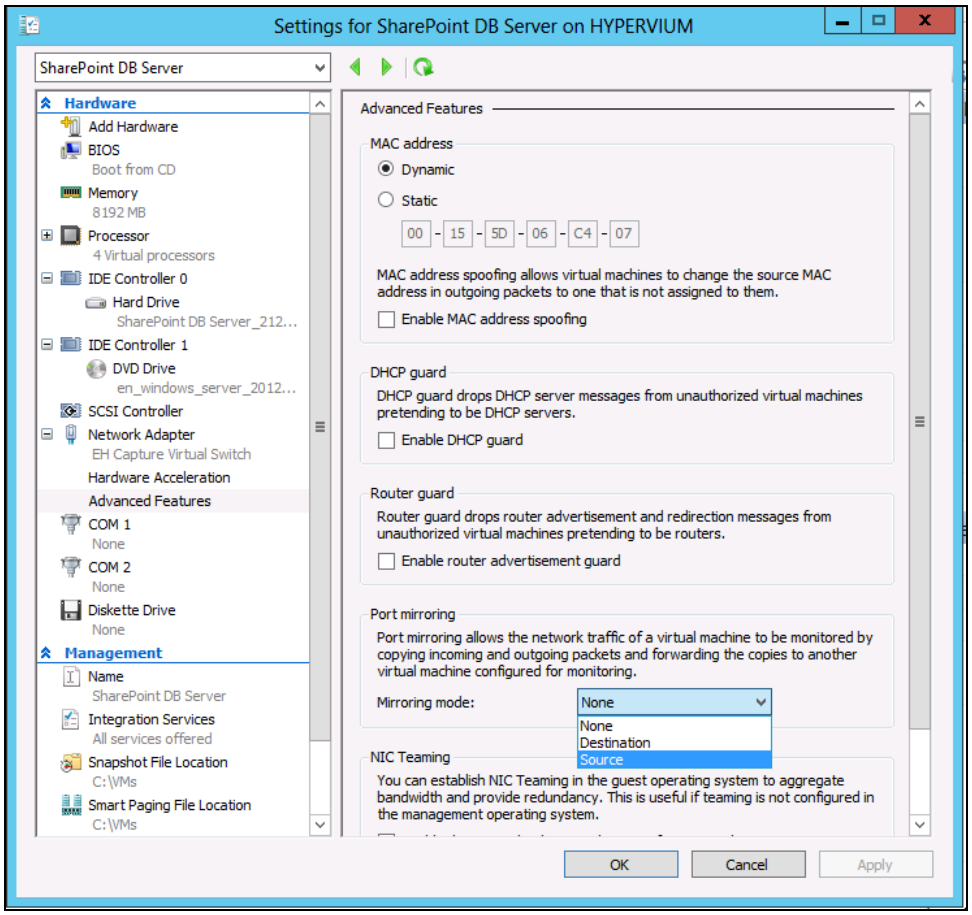
The ExtraHop Discovery Edition can be configured to monitor network traffic of another VM on the same host using Port Mirroring mode in the Hyper-V Manager. An ExtraHop virtual machine running in port mirroring mode can only monitor another virtual machine running on the same virtual switch.

Enabling Port Mirroring Mode in the Hyper-V Manager

1. Right-click the ExtraHop-Discovery VM and select **Settings**.



2. Expand **Network Adapter** and click **Advanced Features**.
3. In the Port mirroring section, click the **Mirroring mode** drop-down list and select **Source**.

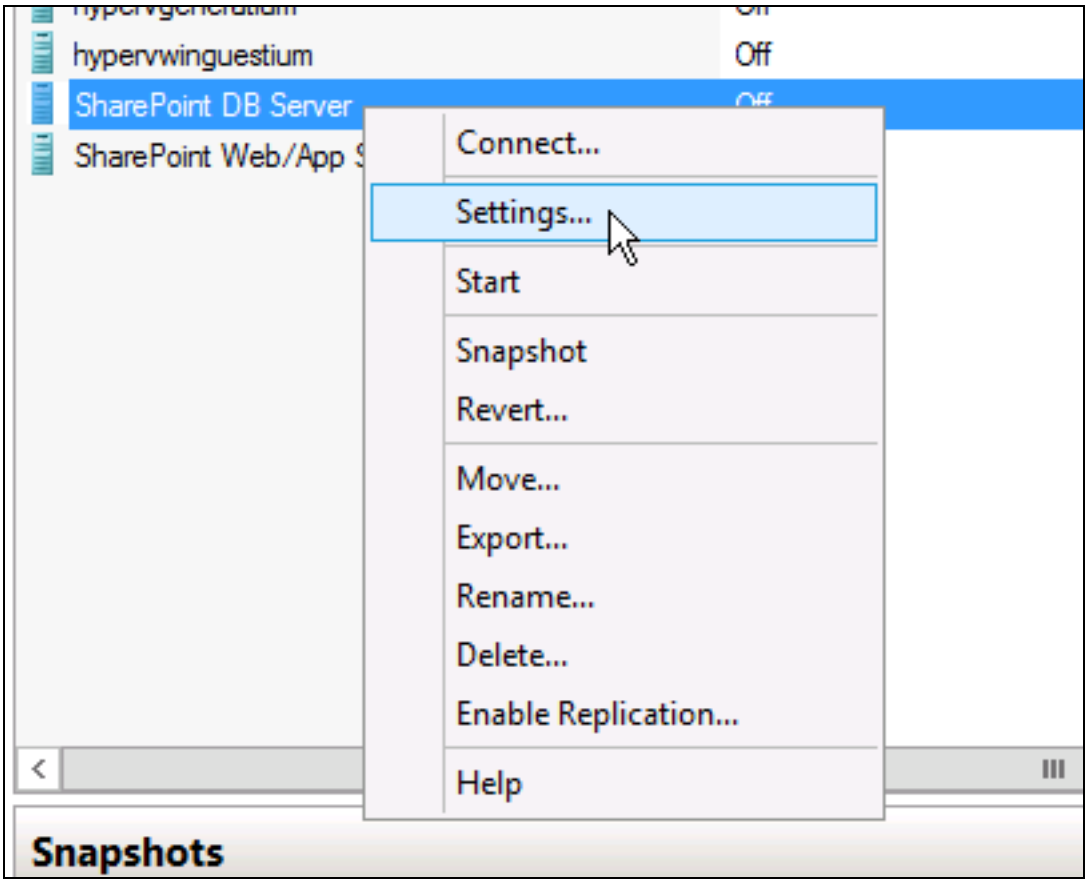


4. Make note of the source network and ensure the ExtraHop system's capture interface is on the same network.
5. Click the **Apply** button.
6. Click **OK**.
7. Repeat these steps for all the VMs you want to monitor, excluding the first VM you created in this procedure.

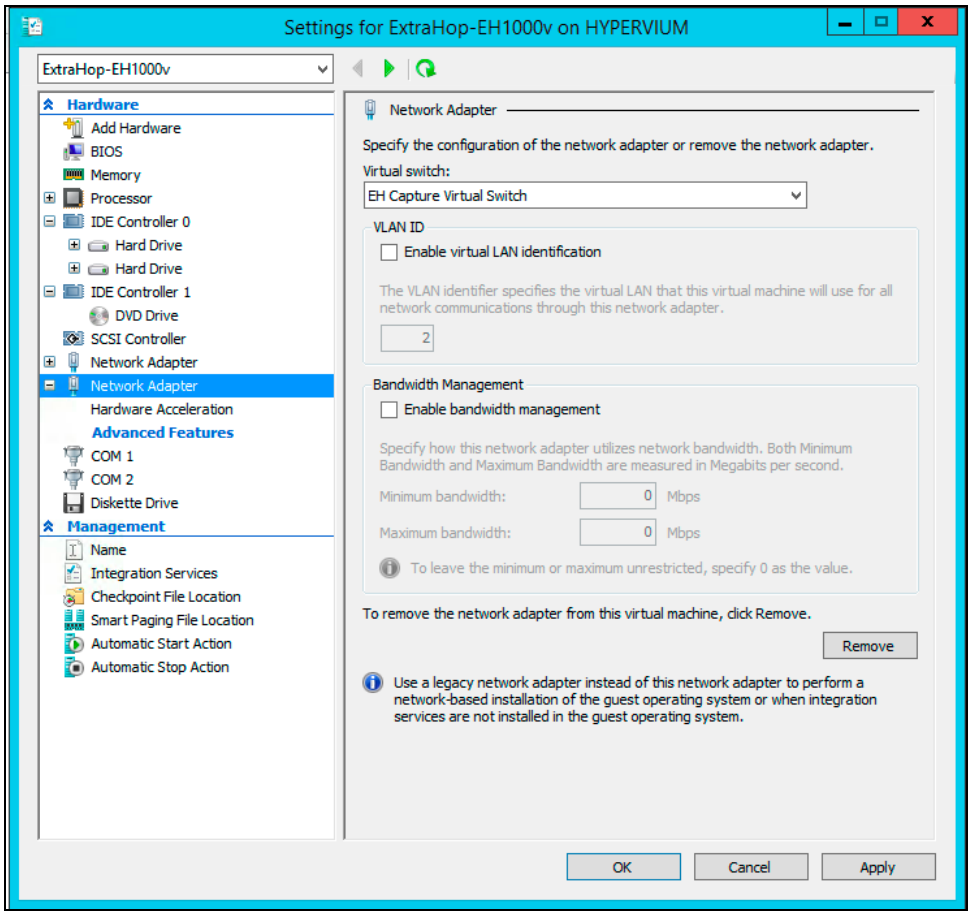
Monitoring External Mirrored Traffic to the VM

This scenario requires a second physical network interface and the creation of a second vSwitch associated with that NIC. This NIC then connects to a mirror, tap, or aggregator that copies traffic from a switch. This setup is useful for monitoring the intranet of an office.

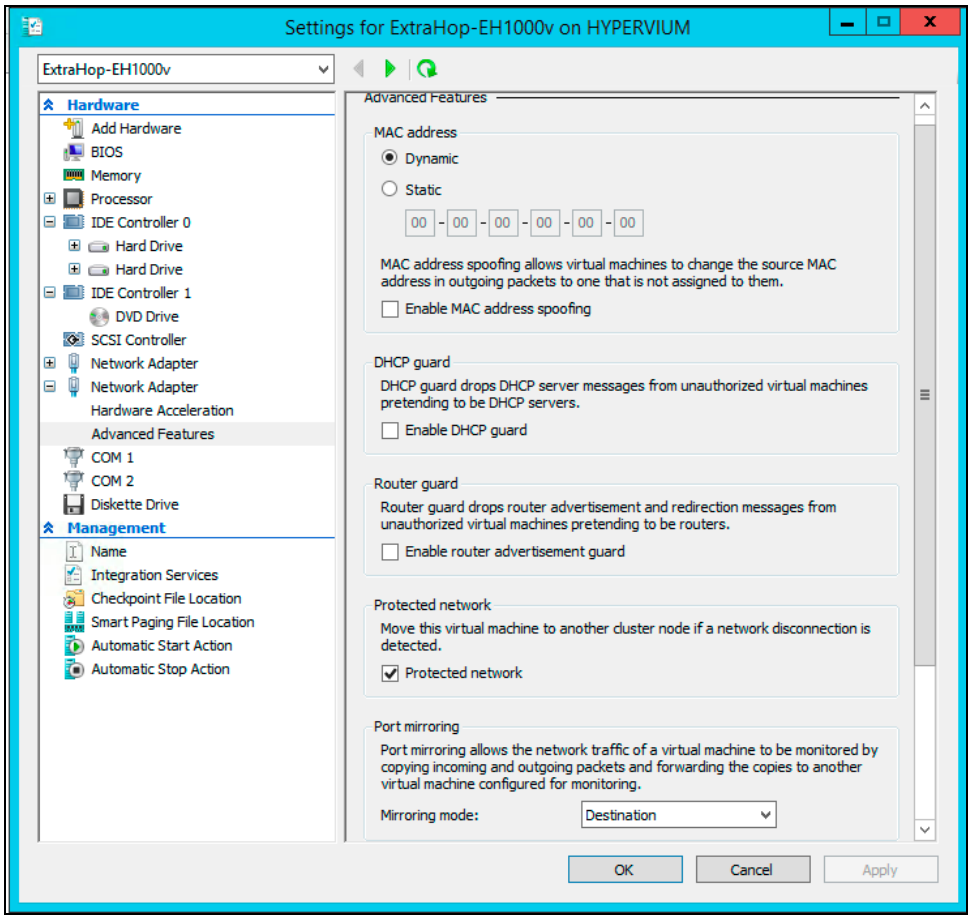
1. Right-click the ExtraHop-Discovery VM and select **Settings**.



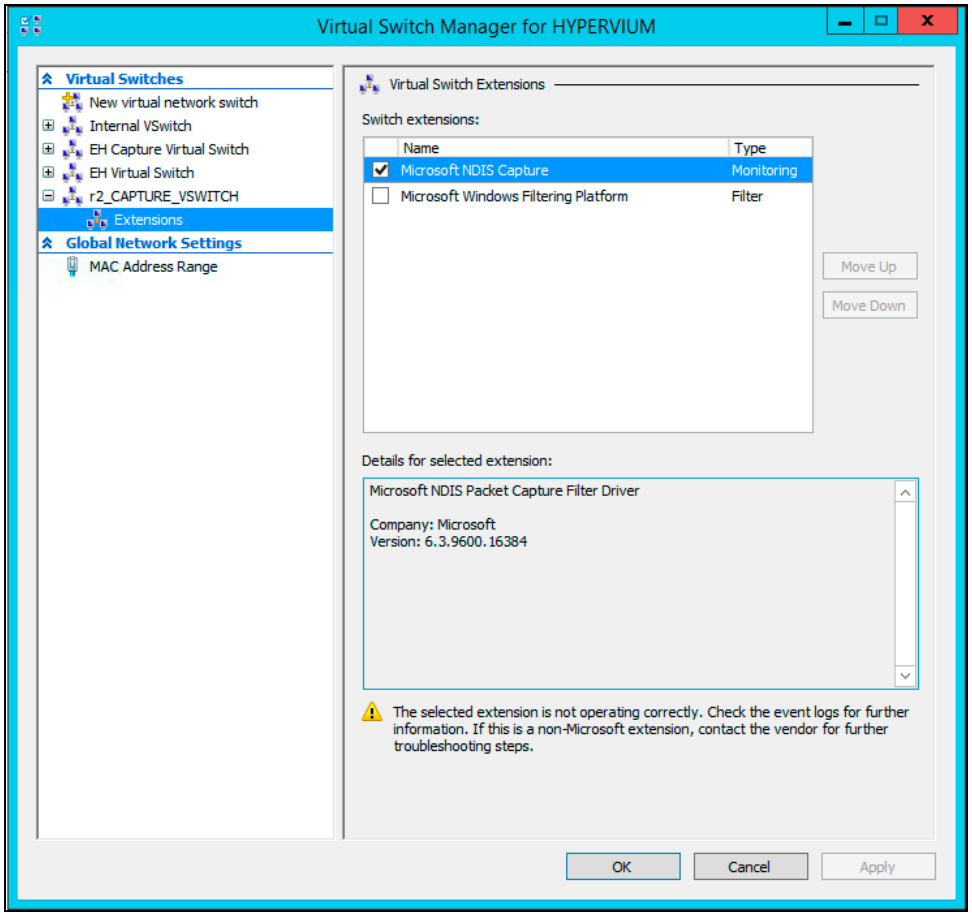
2. Expand **Network Adapter** and click **Advanced Features**.



3. In the Port mirroring section, click the **Mirroring mode** drop-down list and select **Destination**.



4. Click the **Apply** button.
5. Click **OK**.
6. Expand the virtual switch associated with the external data feed and enable the **Microsoft NDIS Capture** switch. Don' t worry about the warning. The PowerShell command in the next step will get it to work.



7. Click the **Apply** button.
8. Click **OK**.
9. Open a PowerShell prompt and enter the following commands:

```
$a = Get-VMSystemSwitchExtensionPortFeature -FeatureId 776e0ba7-94a1-41c8-8f28-951f524251b5
$a.SettingData.MonitorMode = 2
add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName <name of the switch> -VMSwitchExtensionFeature $a
```

Note: This technical reference for this procedure comes from this blog post on the Networking Blog at Technet.

Monitoring Multiple Interfaces on a Windows Server

For servers with multiple interfaces, you can configure the software tap to forward packets from a particular interface or from multiple interfaces by editing its configuration file on the server.

To edit the configuration file, complete the following steps.

1. After installing the software tap, on the server, open the configuration file: C:\Program Files\rpcapd\rpcapd.ini

   The configuration file contains this text or similar:

   ```
   ActiveClient = 10.0.0.100,2003
   NullAuthPermit = YES
   ```

2. Modify the existing ActiveClient line and create an ActiveClient line for each additional interface to be monitored. Specify each interface by its interface name or IP address. For every ActiveClient line, the software tap will independently forward packets from the interface specified in the line:

   ```
   ActiveClient = <extrahop_ip>, <extrahop_port>, ifname=<interface_address>
   ```

   or

   ```
   ActiveClient = <extrahop_ip>, <extrahop_port>, ifaddr=<interface_name>
   ```

   `<interface_address>` specifies the IP address of the interface from which the packets are forwarded. `<interface_address>` may be either the IP address itself, such as 10.10.1.100, or a CIDR specification (network IP address/subnet prefix length) that contains the IP address, such as 10.10.1.0/24.

   `<interface_name>` is the name of the interface from which the packets are forwarded. The name is formatted as `\Device\NPF_{<GUID>}`, where `<GUID>` is the globally unique identifier (GUID) of the interface. For example, if the interface GUID is `2C2FC212-701D-42E6-9EAE-BEE969FEFB3F`, the interface name is `\Device\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}`.

   The following is an example of the configuration file specifying two interfaces using the interface IP address:

   ```
   ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.100
   ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.100
   NullAuthPermit = YES
   ```

   The following is an example of the configuration file specifying two interfaces using CIDR specifications that contain the interface IP address:

   ```
   ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.0/24
   ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.0/24
   NullAuthPermit = YES
   ```

   The following is an example of the configuration file specifying two interfaces using the interface name:

   ```
   ActiveClient = 10.10.6.45, 2003, ifname=\Device\NPF_{2C2FC212-701D-42E6-9EAE-
   BEE969FEFB3F}
   ActiveClient = 10.10.6.45, 2003, ifname=\Device\NPF_{3C2FC212-701D-42E6-9EAE-
   BEE969FEFB3F}
   NullAuthPermit = YES
   ```

3. Save the configuration (.ini) file. Make sure to save the file in ASCII format to prevent errors.

4. Restart the software tap by running the command

```
restart-service rpcapd
```

> **Note**: To reinstall the software tap after changing the configuration file, run the installation command and replace `-RpcapIp` and `-RpcapPort` with the `-KeepConfig` flag in order to preserve the modified configuration file. For example:

```
.\install-rpcapd.ps1 -MgmtIp <extrahop_ip> -KeepConfig
```

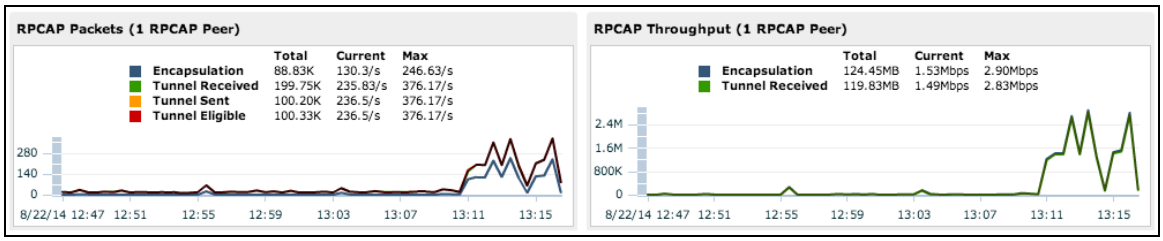
or

```
.\install-rpcapd.ps1 -InputDir . -KeepConfig
```

Analyzing Wire Data from a Software Tap

To find out how much wire data the ExtraHop system is receiving from the software tap:

1. Log in to the ExtraHop Web UI (`https://<extrahop_ip>/extrahop`) and click the **Settings** button.
2. Click **System Health** to get more information about the forwarded traffic. This page displays a Packets and Throughput graph for each software tap connected to the ExtraHop system.



   The RPCAP Packets and Throughput graphs contain four metrics:

   - **Encapsulation**: The total number of RPCAP encapsulation packets received by the ExtraHop system.
   - **Tunnel Eligible**: Total number of packets eligible to be forwarded to the ExtraHop system.
   - **Tunnel Sent**: Total number of RPCAP-tunneled packets forwarded to the ExtraHop system.
   - **Tunnel Received**: Total number of RPCAP-tunneled packets received by the ExtraHop system.

   The tunnel eligible, tunnel sent, and tunnel received values are equal if the ExtraHop system is receiving and processing all the packets sent by the server. If they are not equal, use the following reference for troubleshooting:

   - If **Tunnel Sent** is less than **Tunnel Eligible**, the server is not able to forward all of the traffic. This behavior may indicate that packet forwarding requires more processing or outbound bandwidth resources on the server. Consider separating the forwarding process onto a separate CPU or allocating a dedicated interface for forwarding traffic.
   - If **Tunnel Received** is less than **Tunnel Sent**, the ExtraHop system is not receiving all the traffic forwarded by the server. This behavior may be due to network congestion or insufficient resources on the ExtraHop system. If you suspect it is the latter, contact ExtraHop Support.
3. Once you have verified that the ExtraHop system is receiving traffic, exit the **System Health** page and view metrics in the ExtraHop Web UI.